UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,773	07/25/2001	Michael L. Wenocur	A-70556/RMA	5620

7590 02/23/2005

FLEHR HOHBACH TEST ALBRITTON & HERBERT LLP
Suite 3400
Four Embarcadero Center
San Francisco, CA 94111

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 02/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/912,773	WENOCUR ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/12/02 & 1/8/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-56 are presented for examination.

Claim Objections

Claim 3 is objected to because of the following informalities:

The word "used" has been misspelled. Appropriate correction is required.

Claims 53 and 54 are objected to because of the following informalities:

"know" should be changed to "known". Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 16 recites the limitation "said cipher" in the first line. There is insufficient antecedent basis for this limitation in the claim.

Claim 17 recites the limitation "the cipher" in the first line. There is insufficient antecedent basis for this limitation in the claim.

Claim 19 recites the limitation "said cipher" in the first line. There is insufficient antecedent basis for this limitation in the claim.

Claim 22 recites the limitation "the secret" in the first line. There is insufficient antecedent basis for this limitation in the claim.

Claim 23 recites the limitation "the authentication code" in the first line. There is insufficient antecedent basis for this limitation in the claim.

Claim 35 recites the limitation "the keys" in the first line. There is insufficient antecedent basis for this limitation in the claim.

Claim 38 recites the limitation "said keys" in the first line. There is insufficient antecedent basis for this limitation in the claim.

Claims 43, 45, and 48 recite the limitation "the issuer" in the second line. There is insufficient antecedent basis for this limitation in the claim.

Claim 43 recites the limitation "the session keys" in the second line. There is insufficient antecedent basis for this limitation in the claim.

Claim 44 recites the limitation "the fixed public and private keys" in the first line. There is insufficient antecedent basis for this limitation in the claim.

Claim 44 recites the limitation "the certificate keys" in the second line. There is insufficient antecedent basis for this limitation in the claim.

Claim 46 recites the limitation "the certificate and the keys" in the second line. There is insufficient antecedent basis for this limitation in the claim.

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 44-45 are rejected under 35 U.S.C. 112, first paragraph, as based on a disclosure which is not enabling. "Certificate Key" critical or essential to the practice of the invention, but not included in the claim(s) is not enabled by the disclosure. See *In re Mayhew*, 527 F.2d 1229, 188 USPQ 356 (CCPA 1976).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-6, 11-12, 14-15, 35-38, 40-42, and 49-56 are rejected under 35 U.S.C. 102(b) as being anticipated by Shambroom (U.S. Patent No. 5,923,756 and Shambroom hereinafter).

Regarding claims 1-3, Shambroom discloses a computer program product for use in conjunction with a computer system having a server and a client, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism, comprising: a program module that directs the computer system and/or components thereof including at least one or the client or server, to function in a specified manner to provide message communications the message communications occurring in a computer system hardware architecture neutral and operating system neutral and network transport protocol neutral manner for implementing a plurality of separate security protocols using a common set of criteria, the program module including instructions for:

A. defining two cryptographic primitives (i.e., 1) secret key cryptography and a cipher algorithm 2) transport of the encrypted secret key using public key

cryptography), and B. using only said two cryptographic primitives to construct said plurality of separate security protocols (i.e., client 200 creates a session key, encrypts the session key using one of the cryptographic algorithms indicated by network server 300 in the certificate and the public key sent by network server 300, and sends the encrypted session key to network server 300. After receiving the encrypted session key, network server 300 authenticates itself to client 200 by decrypting this session key and returning to client 200 a message encrypted with the underlying session key)(Col. 7, lines 14-64).

Regarding claims 4-5, Shambroom discloses a method of enhancing security of a message wherein cryptographic primitives include formats and algorithms (i.e., 1) encrypted data using secret key cryptography and a cipher algorithm 2) transport of the encrypted secret key using public key cryptography)(Col. 7, lines 14-64).

Regarding claims 6 and 12, Shambroom discloses wherein cryptographic primitives are for: 1) encrypted data using secret key cryptography and a cipher algorithm 2) transport of the encrypted secret key using public key cryptography (i.e., After receiving the encrypted session key, network server 300 authenticates itself to client 200 by decrypting this session key and returning to client 200 a message encrypted with the underlying session key)(Col. 7, lines 14-64).

Regarding claim 11, Shambroom discloses including data privacy plus integrity using the encryption and data authenticity using a public key digital signature and the certificate chain of the Sender (Col. 7, lines 14-65).

Regarding claim 14, Shambroom discloses wherein the common set of criteria are selected from a set consisting of data formats, algorithms, subroutines, procedures, and combinations thereof (Col. 10, lines 25-67 and Col. 11, lines 1-42).

Regarding claim 15, Shambroom discloses wherein data integrity detection is based on a secret key and a cipher algorithm as cryptographic primitives (Col. 7, lines 14-64).

Regarding claim 35, Shambroom discloses wherein the keys for encryption are derived from exchanged information (Col. 2, lines 6-15).

Regarding claim 36-37, Shambroom discloses wherein the exchanged information is either in clear or in encrypted data (Col. 9, lines 55-67 and Col. 10, lines 1-67 and Col. 11, lines 1-42).

Regarding claim 38, Shambroom discloses wherein the exchanged information provides a form of challenge-response authentication (Col. 5, lines 10-27).

Regarding claim 40-41, Shambroom discloses wherein authentication for a session key is provided by values that are produced by cryptographic hash of some or all of the data transmitted before sending the authenticated message (Col. 8, lines 42-67).

Regarding claim 42, Shambroom discloses wherein separate keys are used by the Sender and Recipient by deriving the keys in different ways from shared information exchanged earlier in the protocol and/or fixed information known to the Sender and Recipient (Col. 9, lines 55-67 and Col. 10, lines 1-67).

Regarding claims 49-51, Shambroom discloses wherein a protocol is implemented to send the public key of the recipient to the sender, in response to a message, where the public key is verified (Col. 7, lines 1-65).

Regarding claims 53-54, Shambroom discloses wherein a protocol is implemented using data encrypted with a secret key known to the recipient that was securely communicated through previous messages (Col. 7, lines 1-65).

Regarding claims 52, 55, and 56, Shambroom discloses wherein a protocol is the set up portion of a bi-directional session (Col. 6, lines 54-67 and Col. 7, lines 1-65).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7-10 and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shambroom (U.S. Patent No. 5,923,756 and Shambroom hereinafter), in view of Ogg et al., (U.S. Publication No. 2002/0178354 and Ogg hereinafter).

Teachings of Shambroom in regards to limitations of claims 2 and 6 have been discussed previously.

Regarding claims 7-10, Shambroom discloses providing privacy and data integrity based on a secret key, from a set comprising a message key and a session key, and a cipher algorithm (Col. 2, lines 52-65 and Col. 7, lines 14-64).

Moreover, Ogg expressly discloses providing privacy and data integrity based on a secret key and any of cipher algorithms of ("RSA") public key encryption, DES, Triple-DES, Pseudo-random number generation, and the like algorithms (Page 2, Par. 0023).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shambroom with the teachings of Ogg by including a secret key and any of cipher algorithms of ("RSA") public key encryption, DES, Triple-DES, Pseudo-random number generation, and the

like algorithms. The motivation for this combination is to provide for a secure system and database that are capable of preventing unauthorized access and tampering (Ogg, Page 1, Par. 0007).

Regarding claims 21-22, Shambroom does not expressly disclose wherein the integrity of the data and associated data tamper detection, is provided by a cryptographic message authentication code that is based on a secret key.

However, Ogg discloses wherein the integrity of the data and associated data tamper detection, is provided by a cryptographic message authentication code that is based on a secret key (Page 19, Par.0 435).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shambroom with the teachings of Ogg by including a cryptographic message authentication code that is based on a secret key. The motivation for this combination is to prevent unauthorized access and tampering (Ogg, Page 1, Par. 0007).

Regarding claim 23, Shambroom does not expressly disclose wherein the authentication code is computed by a CBC-MAC based algorithm and/or a HMAC based algorithm.

However, Ogg discloses wherein the authentication code is computed by a CBC-MAC based algorithm and/or a HMAC based algorithm (Page 19, Par. 0435).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shambroom with the teachings of Ogg by including wherein the authentication code is computed by a HMAC based algorithm. The motivation for this combination is to prevent unauthorized access and tampering (Ogg, Page 1, Par. 0007).

Claims 16-18 and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shambroom (U.S. Patent No. 5,923,756 and Shambroom hereinafter) and Ogg et al., (U.S. Publication No. 2002/0178354 and Ogg hereinafter), in view of Maturana et al., (U.S. Publication No. 2002/0035681 and Maturana hereinafter).

The combined teachings of Shambroom and Ogg with respect to limitations of claims 2, 6, and 7 have been discussed previously.

Regarding claim 16, Shambroom or Ogg does not expressly disclose an Initialization Vector for Cipher-Block-chaining mode that is an input to the primitive and appears in the data format of the output.

However, Maturana discloses wherein the cipher algorithm comprises a block cipher, and the initialization vector primes the algorithm, and is determined as part of the SSL handshake (i.e., by definition, session key is only valid during the session resulted from SSL handshake which means that for the next SSL handshake, the same

process repeats and another initialization vector primes the algorithm)(Page 7, Par. 0064).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Shambroom and Ogg with the teachings of Maturana by including wherein the cipher algorithm comprises a block cipher, and the initialization vector primes the algorithm, and is determined as part of the SSL handshake. The motivation for this combination is to provide a standardized method of adding cryptographic security functions to a TCP-based application such as a web browser (Maturana, Page 1, Par. 0008).

Regarding claim 17, Shambroom discloses wherein the secret key to the cipher is one input to this primitive (Col. 2, lines 35-51).

Regarding claim 18, Shambroom discloses wherein said block cipher is a cipher selected from the set consisting of a triple-DES based cipher, and a XTEA based cipher (Col. 14, lines 27-30).

Regarding claims 24-26, Shambroom discloses implementing an authentication protocol that incorporates the use of timestamps to further enhance the security of the system (Col. 8, lines 1-14).

Neither Shambroom nor Ogg discloses a type, version, or content length field is transmitted before the encrypted data.

However, Maturana discloses the ability to calculate an SSL length, the SSL length is in the SSL header, before sending the first TCP packet (Page 10-11, Par. 0096).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Shambroom and Ogg with the teachings of Maturana by including the ability to calculate an SSL length in the SSL header and send it to the receiver. The motivation for this combination is to eliminate the need to buffer the whole message (Maturana, Page 10-11, Par. 0096).

Claims 13, 27-34, 43, and 46-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shambroom (U.S. Patent No. 5,923,756 and Shambroom hereinafter), in view of Ross, JR., (U.S. Publication 2002/0143885 and Ross hereinafter).

Teachings of Shambroom with respect to limitations of claims 2 and 6 have been discussed previously.

Regarding claim 13, Shambroom discloses wherein security protocols, such as SSL, are used to establish the secure network connection between the client and the network server (Col. 5, lines 10-55).

Moreover, Ross discloses wherein security protocols are selected from the group consisting of: (i) secure interactive sessions, (ii) secure unidirectional messaging, (iii)

secure software downloading, (iv) secure software upgrading, (v) secure issuing of digital certificates, and/or (vi) combinations thereof (Abstract and Page 10, Par. 0137-0157).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shambroom with the teachings of Ross by including security protocols selected from the group consisting of: (i) secure interactive sessions, (ii) secure unidirectional messaging, (iii) secure software downloading, (iv) secure software upgrading, (v) secure issuing of digital certificates, and/or (vi) combinations thereof. The motivation for this combination is to allow for the encryption, sending, receiving, and decryption of e-mail in a heterogeneous network environment (Ross, Page 2, Par. 0018).

Regarding claim 27-29, Shambroom does not expressly disclose providing the software signing, and using a fixed Recipient public key to which all receiving software knows the private key for the encryption.

However, Ross discloses wherein the reader-responder module can be used to send a key from user 102 to the user 304-308 in order to enable the user 304-308 to send an e-mail taking advantage of proprietary features of a first e-mail system (i.e., the email system of user 304-308), to the user 102 who is not on the first email system (Page 10, Par. 0156-0167).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shambroom with the

teachings of Ross by including software signing, and using a fixed Recipient public key to which all receiving software knows the private key for the encryption. The motivation for this combination is to allow for the encryption, sending, receiving, and decryption of e-mail in a heterogeneous network environment (Ross, Page 2, Par. 0018).

Regarding claim 30, Shambroom discloses client 200 (i.e., the sender) creates a session key, encrypts the session key using one of the cryptographic algorithms indicated by network server 300 in the certificate and the public key sent by network server 300, and sends the encrypted session key to network server 300. After receiving the encrypted session key, network server 300 authenticates itself to client 200 by decrypting this session key and returning to client 200 a message encrypted with the underlying session key (Col. 7, lines 14-65).

Regarding claims 31-32, Shambroom does not expressly disclose providing all the security functions required for secure unidirectional messaging.

However, Ross discloses wherein the reader-responder module can be used to send a key from user 102 to the user 304-308 in order to enable the user 304-308 to send an e-mail taking advantage of proprietary features of a first e-mail system (i.e., the email system of user 304-308), to the user 102 who is not on the first email system (Page 10, Par. 0156-0167).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shambroom with the

teachings of Ross by including the security functions required for secure unidirectional messaging. The motivation for this combination is to allow for the encryption, sending, receiving, and decryption of e-mail in a heterogeneous network environment (Ross, Page 2, Par. 0018).

Regarding claim 33, Shambroom discloses wherein a session key is set up between sender and receiver where the sender knows the recipient's public key (Col. 7, lines 14-65).

Regarding claim 34, Shambroom discloses wherein the sender knows the recipient's public key by receiving it in the previous communications (Col. 7, lines 14-65).

Regarding claims 43, 46-47, Shambroom discloses client 200 creates a session key, encrypts the session key using one of the cryptographic algorithms indicated by network server 300 in the certificate and the public key sent by network server 300, and sends the encrypted session key to network server 300. After receiving the encrypted session key, network server 300 authenticates itself to client 200 by decrypting this session key and returning to client 200 a message encrypted with the underlying session key (i.e., sending a resource tag to the issuer after the session keys have been established)(Col. 7, lines 14-65).

Regarding claim 48, Shambroom does not expressly disclose wherein the certificate issuing is further authenticated using fixed public and private keys for the client device that wants to get a certificate from the issuer.

However, Ross discloses program code means for enabling the computer to open by the second user the attachment to execute the reader/responder software application program including program code means for enabling the computer to allow a user without the email client software to read and respond to encrypted email created and sent from a user having the email client software (i.e., note that any user who is going to use first user's email system is sent the same unencrypted public key along with the reader/responder software application)(Page 4-5, Par. 0036).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shambroom with the teachings of Ross by including fixed public and private keys for the client device that wants to get a certificate from the issuer. The motivation for this combination is to allow for the encryption, sending, receiving, and decryption of e-mail in a heterogeneous network environment (Ross, Page 2, Par. 0018).

Claims 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shambroom (U.S. Patent No. 5,923,756 and Shambroom hereinafter) and Ogg et al., (U.S. Publication No. 2002/0178354 and Ogg hereinafter), in view of Medvinsky, (U.S. Publication 2002/0094081 and Medvinsky hereinafter).

The combined teachings of Shambroom and Ogg with respect to limitations of claims 2, 6, and 7 have been discussed previously.

Regarding claims 19-20, Shambroom or Ogg does not expressly disclose wherein the cipher algorithm comprise a stream cipher, such as an RC4 cipher type without an Initialization Vector, the bytes of the key are not reused, and the secret key to the cipher is one input to this primitive.

However, Medvinsky discloses wherein the cipher algorithm comprise a stream cipher, such as an RC4 cipher type without an Initialization Vector, the bytes of the key are not reused, and the secret key to the cipher is one input to this primitive (Page 1, Par. 0001-0005).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Shambroom and Ogg with the teachings of Medvinsky by including wherein the cipher algorithm comprise a stream cipher, such as an RC4 cipher type without an Initialization Vector, the bytes of the key are not reused, and the secret key to the cipher is one input to this primitive. The motivation for this combination is to enable sender and receiver key streams to be synchronized (Medvinsky, Page 1, Par. 0005).

Allowable Subject Matter

Claim 39 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Howard, Jr. et al., (U.S. Patent No. 6,442,690),

Micali, (U.S. Patent No. 5,537,475),

Riggins, (U.S. Patent No. 6,233,341), and

Spelman et al., (U.S. Patent No. 5,638,445).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A. Sherkat

Arezoo Sherkat
Patent Examiner
Group 2131
Feb. 18, 2005

Gregory J. Lamarre
Primary Examiner